Research Paper | Information Tech. | E-ISSN No : 2454-9916 | Volume : 9 | Issue : 6 | June 2023

CYBER-CRIME AND OTHER CYBER SECURITY THREATS IN THE US

Jonathan Chan

Research Scholars Program, Harvard Student Agencies, In collaboration with Learn with Leader

ABSTRACT

This paper provides an overview for one of the most prevalent topics in the tech industry: cybercrime. The paper first discusses the basic concepts and examples of cybercrime, such as social engineering attacks as well as DDoS. The paper also goes through noteworthy cyber-crime incidents which happened in recent times, including the SolarWinds attack. Lastly, the paper proposes ways the US government can deal with these problems, such as the 'zero-trust model.'

KEYWORDS: Cyber-Crime, Ransomware, Malware, Data Theft, Privacy.

INTRODUCTION

Cybercrime, referred to as 'crime that is committed using the internet' according to the Oxford dictionary, is an ever-present and growing threat in today's society. In the US, data compromises have increased almost 12 times as much in 2021 compared to 2005. In the first half of 2022, over 53 million individuals were affected by data breaches. (Statista, 2022) Through the use of computers and the internet, Cybercrime is not only one of the main perpetrators of identity and data theft, but also a danger to the economy, where in 2015, it was estimated that the annual cost to the global economy was over 300 billion euros. (Armin, 2015) Despite this, cybersecurity systems struggle to keep up with the growing rates of cyber-crime. Cyber-security threats in the US should be taken more seriously and we need to develop stronger and more effective ways to counter this problem as they may be dangerous and harmful to privacy and other issues in society.

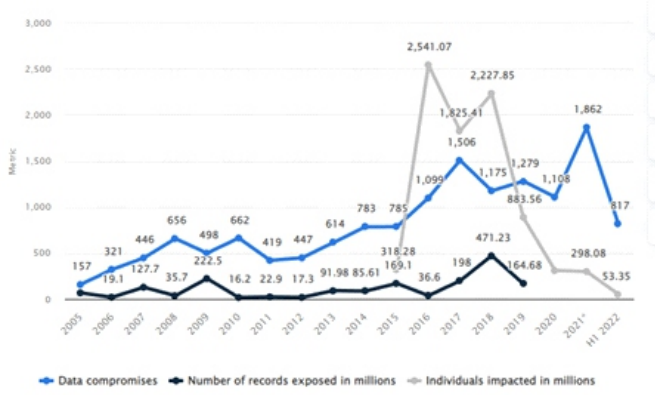

Figure 1: Annual number of data compromises and individuals impacted in the United States between 2005-2022
Source: Statista.com

Methodology

In this research article on the topic "Cyber-crime and other cyber security threats in the US," secondary research serves as the primary research method, utilizing tools such as Google Scholar. The choice of secondary research is driven by the extensive existing discussions and analysis of concepts and data related to the subject matter. However, some primary research is incorporated, including consultations with professionals from the computer science department at a high school. The research process began by dividing the paper into sections, such as an examination of cyber-crime issues and the provision of relevant examples. This approach facilitated focused and efficient research, ensuring the collection of pertinent information. The data primarily originates from reputable sources such as Forbes, the CISA (Cybersecurity and Infrastructure Security Agency), and the GAO (Government Accountability Office).

Discussion & Results

Cyber-attacks range from different sizes, but a common form of a cyber-attack could be in the form of a malware attack. At the very basic level, perpetrators can use a method called 'phishing' to steal data from victims. This involves using 'fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside.' (University of North Dakota, 2020). Sometimes, the act of simply clicking on the email is enough to harm the victim as the user's computer may be redirected to a fake website, leading to a data breach. Another type of a cyber-attack may be spyware, which involves firstly granting the perpetrator access to the computer system itself, then allowing the perpetrator the ability to record 'keystrokes, screenshots, authentication credentials…and other personal information' without the user's consent. This confidential information is then sold to other 'online attackers', or even organizations who may use this information for financial and marketing purposes (University of North Dakota, 2020). DoS, or DDoS attacks, which stands for denial of service/distributed denial of service aims to overload a particular computer or network with information and data until it 'cannot respond to requests'. Through this, online attackers are able to exploit this weakness in the network to launch further attacks to cause more damage (University of North Dakota, 2020).

At a larger scale, these attacks may involve crimes such as data theft, blackmail, and extortion to a more serious degree. On the 13th of December, 2020, FireEye, a cybersecurity company announced the finding of a 'cyber intrusion' within a software application developed by the SolarWinds company (GAO, 2021). The operation involved firstly the infiltration of the supply chain of the company, which then is utilized by cyber-criminals to send out trojan horses (malicious code disguised as harmless code or software) in the form of a patch for their software product and as a result, according to the U.S Government Accountability Office, it is estimated that close to '18,000' users received a software update for their SolarWinds software product (GAO, 2021).

'Karakurt', a newer online crime group has been coming to focus recently in the US for cyber extortion. Rather than using ransomware, a type of malware which encrypts victim's data into unreadable code then demands a ransom for the decryption key, the organization steals data through other methods such as obtaining stolen credentials from third parties or exploiting intrusion vulnerabilities. 'Karakurt' will ask for a ransom payment for the data, ranging from $25,000 to $13,000,000 in the past. Otherwise, sensitive data is often auctioned/released to the public via the Dark Web, damaging and exposing the privacy and personal information of victims (CISA, 2022) The Cybersecurity and Infrastructure Security Agency of the United States further claims that 'As of May 2022, the website contained several terabytes of data purported to belong to victims across North America and Europe.'

According to the Pew Research Center, in 2014, Americans have very little confidence in their data privacy online, where only 31% of adults felt at least 'somewhat confident' in government agencies being able to maintain their data securely and privately, while just 9% of adults felt 'very confident' in credit card companies doing the same thing (Madden & Rainie, 2020). In 2016, 35% of US adults had been notified of some kind of sensitive information being compromised, and 14% of US adults had someone impersonate them to attempt taking out loans or lines of credit (Madden & Rainie, 2020). As cyber-attacks and data breaches on governments and private businesses became increasingly common, it was evident that at the time, the US needed to develop more effective ways to deal with this growing concern. Currently in September 2022, the Department of Homeland Security announced a cyber-security grant program across the local, state and territorial governments of the US. This $1 billion funding serves to help governments address future cybersecurity risks as well as improve current cybersecurity infrastructure and systems, but is this enough?

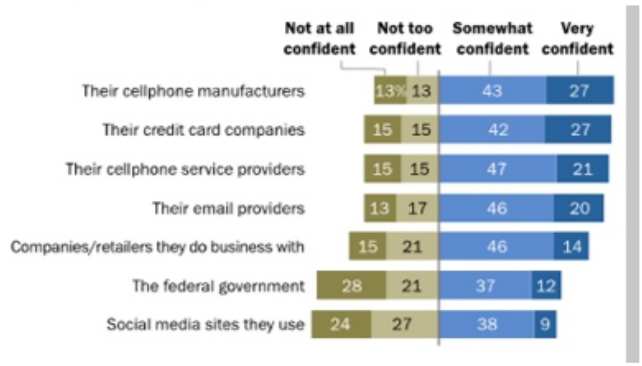

Figure 2: Percentage of US adults/tech users who are confident in the ability of the following institutions to protect their data
Source: Pew Research Center (2019)

For many Americans, cybercrime and their security online is not a large concern for them and many of them 'do not express profound worries' about these issues in their personal lives (Madden and Rainie, 2020). Despite this, many Americans seem lack knowledge and awareness of online threats, where almost 12% of Americans have tried to open a phishing link in 2020 (O'Driscoll, 2022). Meanwhile in the same year, only 52% of US workers know the definition of phishing, and just 54% know the meaning of malware (Kulikova, 2021). Presently, the US government plans on launching 'pilot programs' which aims to 'educate the public about the security of the software sold to the government.' (Purdy, 2021).

It is recommended that the US government extend this education program further, with the aim to inform Americans about current cybersecurity threats, as well as ways to avoid them. Furthermore, the US government needs to increase the monitorization of programs and products for cyber-threats or other 'red flags.' Currently, the federal government employs a 'zero-trust model' (White House, 2022) **only** for firms working with the government to continuously check for suspicious activity, such as 'whether information is being accessed from an unknown IP address.' It is recommended that the government expand this policy to all companies in the country to ensure maximum national and economic security.

CONCLUSION

To conclude, modern cyber threats come in many different forms and the US government can use a range of methods in countering these threats, such as investments into education about online security as well as implementing specific policies. As society enters a grater technological era, we get more intertwined and connected to the internet; and as the online world continues to develop, online threats and attacks grow stronger as well. As one of the leading countries in computers and technology, the US needs to continue making strides in developing new ways to keep up with the constantly evolving threats.

REFERENCES

1. Purdy, Andy. "Council Post: The US Needs a Stronger Commitment to Cybersecurity." Forbes, Forbes Magazine, 30 July 2021, https://www.forbes.com/sites/forbestechcouncil/2021/07/30/the-us-needs-a-stronger-commitment-to-cybersecurity/?sh=76ca627f5daf.
2. Expert Panel. "14 Emerging and Ongoing Cyberthreats Every Organization Needs to Be Aware Of." Forbes, 12 Aug. 2022, www.forbes.com/sites/forbestechcouncil/2022/08/12/14-emerging-and-ongoing-cyberthreats-every-organization-needs-to-be-aware-of/?sh=655e632a1deb.
3. Koziol, Jack. "Most Common Cyber Security Threats in 2022." Forbes Advisor, 12 Aug. 2022, www.forbes.com/advisor/business/common-cyber-security-threats.
4. University of North Dakota. "7 Types of Cyber Security Threats." University of North Dakota Online, 2 Oct. 2020, onlinedegrees.und.edu/blog/types-of-cyber-security-threats.
5. "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (Infographic)." U.S. GAO, (2021) www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.
6. Olmstead, Kenneth, and Aaron Smith. "Americans and Cybersecurity." Pew Research Center: Internet, Science & Tech, 15 Sept. 2022, www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity.
7. Mary Madden, Lee Rainie. "Americans' Attitudes About Privacy, Security and Surveillance." Pew Research Center: Internet, Science & Tech, 17 Aug. 2020, www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance.
8. Kulikova, Tatyana. "Spam and Phishing in 2020." Securelist, 28 Apr. 2021, securelist.com/spam-and-phishing-in-2020/100512.
9. Aimee O'Driscoll. "30+ US Cyber Security and Cyber Crime Statistics (2022)." Comparitech, 8 July 2022, www.comparitech.com/blog/information-security/us-cyber-crime-statistics.
10. White House. "30+ US Cyber Security and Cyber Crime Statistics (2022)." Comparitech, 8 July 2022, www.comparitech.com/blog/information-security/us-cyber-crime-statistics.
11. Armin, Jart. "2020 Cybercrime Economic Costs: No measure No solution. 2015, https://www.cyberroad-project.eu/m/filer_public/2016/05/03/armin_ares2015.pdf, PDF file.
12. Statista. "Cyber Crime: Number of Compromises and Victims in U.S. 2005-H1 2022." Statista, 31 Aug. 2022, www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed.]
13. Cybersecurity and Infrastructure Agency. "Alert (AA22-152A) Karakurt Data Extortion Group (2022)." CISA, 1 June 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-152a